1. Владимиров В. В., Лаппо Г. М. Исследование экологических проблем городских агломераций // Экологические аспекты городских систем. – М.: Наука, 1984. – С.16.

Отримано 16.01.2002

УДК 004.056.55

В.Б.УФИМЦЕВА
Харьковская государственная академия городского хозяйства

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Анализируются криптографические методы защиты информации в системах управления городским хозяйством. Проводится оценка наиболее распространенных современных криптографических систем (DES, ГОСТ 28147-89, RC5 и RSA) и относительно новых криптоалгоритмов - финалистов конкурса на звание нового криптостандарта AES - MARS, RC6™, Twofish, Serpent и самого стандарта AES - Rijndael. Даются рекомендации по разработке новых методов защиты информации.

Использование информационных систем в управлении городским хозяйством приводит к необходимости защиты информации от несанкционированного доступа, умышленного изменения, кражи, уничтожения и других преступных действий. Различают два основных требования к системам защиты информации: сохранение конфиденциальности и целостности данных. Наиболее эффективным средством защиты информации, позволяющим решать обе эти задачи (конфиденциальности - путем лишения противника возможности извлечь информацию, и целостности - путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию), является криптографическое ее преобразование.

1. Классификация криптографических методов

По количеству и способу передачи ключей

В классической *симметричной (одноключевой) криптографической системе* шифрация путем обратимого преобразования E_k и дешифрация сообщения происходят с помощью одного и того же секретного ключа K. Основным недостатком такой системы является необходимость передачи секретного ключа по несекретному каналу [1]. Избежать этого недостатка позволяют *криптосистемы с открытым ключом*. В такой системе генерируются два ключа. Один – секретный ключ K_c – остается у получателя, а открытый ключ K_o передается по несекретному каналу или наоборот. Концепция асимметричных криптографических систем основана на применении однонаправленных функций (дискретное возведение в степень, целочисленное умножение, комбинаторные задачи и др.). Недостатками метода являются

сложность вычислений, вследствие чего значительно увеличивается время, необходимое для шифрации-дешифрации, и возможность нахождения эффективного метода решения обратных задач, что приведет к полной открытости шифра.

По способу представления исходного сообщения

Поточное шифрование состоит в том, что текст открытого сообщения последовательно складывается с ключом в виде псевдослучайной последовательности чисел, создаваемой генератором. К достоинствам поточных шифров относятся эффективность и быстродействие, относительная простота реализации и отсутствие размножения ошибок. Недостатками являются необходимость синхронизации использования одной и той же ключевой последовательности для шифрации и дешифрации, что приводит к нарушению криптостойкости системы, и невозможность использования для аутентификации информации.

При *блочном шифровании* открытый текст сначала разбивают на равные по длине блоки, затем применяют зависящую от ключа функцию шифрования. Достоинством метода является то, что два блока открытого текста не могут быть представлены одинаковыми блоками шифртекста. Алгоритм блочного шифрования может быть использован в двух режимах: *прямом* (каждый из блоков открытого текста шифруется независимо от других, однако фиксированная длина блоков позволяет осуществить криптоанализ "со словарем" в ограниченной форме и метод не предусматривает аутентификацию данных) и *сверточном* (функция шифрования зависит не только от ключа, как при прямом блочном шифровании, но и от одного или более предшествующих блоков шифртекста. Достоинствами являются возможность обнаружения манипуляции данными (при этом используется факт размножения ошибок) и аутентификации данных, а недостатком - сложность разработки и реализации таких систем по сравнению с прямым блочным шифрованием.

По способу шифрования

Шифрование перестановкой характеризуется простотой алгоритма и возможностью программной реализации, но низким уровнем защиты, так как при большой длине сообщения в криптограмме проявляются статистические закономерности ключа, что позволяет его быстро раскрыть.

Шифрование подстановкой. При *одноалфавитном шифровании* каждый символ исходного текста заменяется символом того же алфавита на всем протяжении текста. Достоинство метода заключается в простоте реализации, однако одинаковые статистические характеристики исходного алфавита и алфавита шифра повышают вероятность

успешного вскрытия шифра.

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. В компьютерной криптографии часто используется шифр Вернама на основе операции "исключающее ИЛИ". Эффект использования многоалфавитных подстановок заключается в том, что обеспечивается маскировка естественной статистики исходного языка, но при использовании компьютера эти шифры легко вскрываются даже при большой длине ключа.

Шифрование заменой на основе аналитических преобразований заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Эти методы обеспечивают надежное шифрование, реализуются программно (при этом часто один алгоритм используется и для шифрации, и для дешифрации), однако для шифрации и дешифрации требуется выполнить сложные арифметические действия, что приводит к увеличению времени обработки информации, и объем ключа существенно увеличивается с ростом размера кодирующей матрицы.

Избежать этих недостатков позволяет *метод на основе матриц Стахова* [2]. Этот метод заключается в умножении исходного текста, представленного в виде квадратной матрицы M размером $(p+1)\times(p+1)$ на n-ю степень матрицы Стахова p-го порядка Q_p^n, а дешифрация состоит в умножении матрицы криптограммы C на обратную матрицу Стахова Q_p^{-n}. При этом особые свойства матриц Стахова сводят процесс умножения и возведения в степень матриц к простым операциям сложения или вычитания, а для передачи матрицы кода требуется передача только двух чисел p и n.

Детерминант матрицы Q_p^n равен $(-1)^{pn}$, поэтому детерминант матрицы исходных данных может отличаться от детерминанта матрицы криптограммы лишь знаком, что позволяет не только обнаружить ошибки в полученных данных (без предварительного расшифровывания), но и во многих случаях исправить ее.

Этот метод при возможности аутентификации информации и исправления ошибок требует выполнения простых арифметических операций. Однако умножение на матрицу Стахова является линейной операцией, поэтому для обеспечения секретности метода вид матриц необходимо хранить в секрете, что противоречит правилу Керкоффа. Длина ключа определяется размером чисел для задания ранга p и степени матрицы n, поэтому они должны быть достаточно большие, а даже сравнительно небольшие величины p и n приводят к значительной избыточности информации за счет операции умножения матриц и

увеличения детерминанта матрицы исходного текста.

Шифрование методом гаммирования заключается в наложении гаммы шифра (псевдослучайная последовательность, выработанная по заданному алгоритму) на исходный текст обратимым способом. Получаемый таким методом шифртекст довольно трудный для раскрытия, имеет высокую скорость обработки данных исключает возможность размножения ошибки, однако период гаммы ключа должен быть достаточно большим для шифрования сообщений различной длины.

Комбинированные шифры заключаются в последовательном использовании простых шифров, что позволяет не только придерживаться двух основных принципов Шеннона - рассеивания и перемешивания, но и обеспечивать легкость шифрования и расшифрования при известном пользователю ключе. Чаще всего в качестве простых шифров используют перестановки и замены.

2. Современные криптографические системы

Американский стандарт шифрования данных DES - это симметричная блочная криптосистема, имеющая структуру сети Фейстеля [3]. DES осуществляет шифрование 64-битовых блоков данных и ключа, в котором значащими являются 56 бит. Алгоритм используется в четырех рабочих режимах: электронная кодовая книга ECB, сцепление блоков шифра CBC, обратная связь по шифртексту CFB и обратная связь по выходу OFB. К достоинствам DES алгоритма можно отнести достаточно высокий уровень защиты при достаточной простоте алгоритма, широкое распространение, экономичность в реализации и эффективность в быстродействии. Однако при таком размере ключа алгоритм может быть взломан методом грубой силы, а S-блоки, на которых основана стойкость системы, не оптимизированы против линейного криптоанализа. DES имеет слабые ключи, что способствует криптоанализу и является недостатком при использовании алгоритма в виде хэш-функции. Использование "тройного" DES с тремя различными ключами приведет к снижению в три раза быстродействия алгоритма.

Криптосистема RC5-w/r/b характеризуется переменными величинами входного блока 2w, числа раундов r и длины ключа b, однако эти параметры являются фиксированными для определенной модификации. Шифрование заключается в поочередном преобразовании подблоков w с использованием операций поразрядного суммирования по модулю 2, суммирования по модулю 2^w и управляемых данными операций циклического сдвига. Непредопределенность операций преобразования данных обеспечивает высокую стойкость алгоритма к ли-

нейному и дифференциальному анализу, однако теоретические атаки основывались на том, что циклический сдвиг не влияет на все биты в регистре.

Алгоритм преобразования данных по ГОСТ 28147-89 представляет собой 64-битовый блочный алгоритм с 256-битовым ключом и предусматривает четыре режима работы: шифрование данных в режиме простой замены; шифрование данных в режиме гаммирования; шифрование данных в режиме гаммирования с обратной связью; выработка имитовставки. К достоинствам метода относится большой размер ключа, однако метод имеет относительно низкое быстродействие и таблицы перестановок рекомендуется держать в секрете, что противоречит требованию открытости криптоалгоритма.

Криптосистема шифрования данных RSA с открытым ключом может работать в режиме шифрования данных и в режиме цифровой подписи. Безопасность алгоритма RSA базируется на трудности решения задачи факторизации больших чисел, являющихся произведением двух больших простых чисел. Однако из-за сложности операций над большими числами программная реализация RSA примерно в 100 раз медленнее реализации DES, а также возможность нахождения эффективного обратного преобразования может привести метод к полной незащищенности.

В 1997г. Национальный институт стандартов и технологий NIST США объявил конкурс среди симметричных криптоалгоритмов на звание криптографического стандарта AES (Advanced Encryption Standard). В финал вышли пять алгоритмов: *MARS* имеет несколько уровней: первоначальные и конечные отбеливание и безключевая перестановка и 8 раундов преобразования с ключом с использованием S-блоков; *криптосистема RC6™*, созданная на основе RC5, является преобразованной сетью Фейстеля для четырех подблоков и использует циклический сдвиг по функции от данных $x\times(2x+1)$, начальное и конечное отбеливание и перестановку подблоков для увеличения лавинного эффекта; *Rijndael* является сетью преобразования линейной заменой с 10, 12 и 14 раундами в зависимости от размера ключа, блок данных рассматривает как матрицу битов, использует линейные перестановки строк и столбцов матрицы и S-блоки; *Serpent* также является сетью преобразования линейной заменой, использует начальную и конечную безключевые перестановки, операцию XOR с ключом, линейные перестановки и S-блоки; *Twofish* является сетью Фейстеля, измененную использованием 1-битового сдвига, и основан на использовании зависящих от ключа S-блоков, псевдоадамарового преобразования и операции XOR с ключом.

Ни один из финалистов, по мнению NIST, не является "идеальным" AES, однако ни один из них не был дискредитирован по отборочным критериям (криптостойкость, быстродействие, возможность реализации в различных приложениях и т. д.), однако в определенных приложениях из-за требования универсальности они могут уступать по некоторым критериям более специализированным криптоалгоритмам. После сравнительного анализа в качестве AES был выбран криптоалгоритм Rijndael [4].

Таким образом, для сохранения конфиденциальности и целостности информации больших объемов (по сравнению с 64-битовым блоком) целесообразно использовать преимущества высокоскоростной работы, присущие симметричным криптосистемам с секретным ключом. Для усложнения (предотвращения) криптоанализа, которому для работы требуются блоки открытого текста и шифртекста, необходимо создать систему с переменной длиной блока, зависящей от ключа шифрования. Такая система, отвечающая всем требованиям, предъявляемым к алгоритмам шифрования данных, может быть построена на основе комбинирования простых методов перестановки и замены: метода перестановки, метода Вернама на основе операции XOR и управляемой операции циклического сдвига (аналогично системам RC5 и RC6™) для обеспечения стойкости алгоритма к линейному и дифференциальному анализу и системы на основе матриц Стахова для обеспечения аутентификации данных. При этом для шифрования, передачи и последующего расшифрования только секретного ключа или другой ценной информации небольшого объема можно использовать криптосистему в режиме исправления ошибок.

1.Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.

2.Stakhov A. P., Massingue V., Sluchenkova A. Introduction into Fibonacci coding and cryptography. - Kharkiv: Osnova, 1999. – 236 c.

3.Schneier B. Applied Cryptography. - John Wiley & Sons, Inc., 1996. – 758 p.

4.Report on the Development of the Advanced Encryption Standard (AES)/ J. Nechvatal, E. Barket, L. Bassham, W. Burr, M. Dworkin, J. Foti and E. Roback, October 2000.

Получено 22.01.2002